MINNESOTA STATE **STANDARD**

From the Office of Carolyn Parnell
Chief Information Officer, State of Minnesota

Version: 1.00
Approved Date: 4/29/2011
Approval: Signature on file

Enterprise Security Patch Management Standard

Standard Statement

Government entities must maintain all supported platforms to an appropriate patch level that maintains the risk exposure of the platform and environment to an acceptable level. Patching processes must:

- Maintain a current inventory of system components, hardware, and software that require patching
- Test patches prior to prevent the introduction of additional vulnerabilities or weakness
- Approve patches prior to deployment that explicitly accepts any residual security risks
- Deploy security patches in accordance with security risk tolerances based on the potential impact
- Test security patches after deployment to ensure remediation of security risk
- When possible, employ automated mechanisms to test, deploy, and validate patches

Reason for the Standard

Patch management supports a number of security practices in addition to other operational activities that help mitigate the exploitation of known security vulnerabilities. Well defined patch management processes help prevent the introduction of problems into an environment and prepares for things going wrong due to changes

This standard specifies the requirements for the implementation of information security patch management process controls for information systems and assets in order to reduce the likelihood of a security breach due to unmaintained environments or reintroduction of known vulnerabilities. It encompasses information systems for which government entities have administrative responsibility, including systems managed or hosted by third-parties on the agencies' behalf.

Roles & Responsibilities

Office of Enterprise Technology (OET)

- Maintain this document
- Work with government entities to develop platform specific configuration guidelines
- Fulfill the Government Entity role and responsibilities for OET

Government Entity

- Ensure that third party contracts are in compliance with this standard
- Review and revise baseline configurations at least annually
- Maintain a change control process
- Periodically report configuration compliance for priority 1 and 2 systems to the enterprise security office

Applicability and Exclusions

This standard is applicable to all government entities in the Executive Branch of state government that manage systems that handle, store, or transfer government data, as identified within the Enterprise Security Applicability Standard. It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on security incidents must be aware of this standard

This requirements of this standard must be incorporated into agreements with third parties to ensure proper notification of information security incidents and their impact on state information assets.

Regulatory, Policy, Standards, & Guideline References

Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)

Minnesota Statutes, Chapter 13 (Data Practices Act)

Enterprise Information Security Operational Control Policy – Configuration and Patch Management Policy

Forms, Templates, and Procedures

Italicized terms can be found in the Enterprise Security Glossary of Terms

Compliance

Compliance with this standard is required within 1 year of the approval date of the standard.

History

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #
05/04/2011	Neal Dawson	Initial Release	1	0

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date
SME	Chris Buse Review & Approval	2/22/2011
ISC	Information Security Council Approval	3/2/2011
CIOC	CIO Council Approval	4/28/2011